REMARKS

Claim 1-19 were examined by the Office, and in the final Office Action of April 11, 2008 all claims are rejected. With this response claims 1, 7, 13-14 and 16-18 are amended, and claims 3, 9 and 15 are cancelled. All amendments are fully supported by the specification as originally filed. Support for the amendments can be found at least from cancelled claims 3, 9 and 15, as well as page 8, lines 21-22 and page 11, line 28—page 12, line 22 of the specification. Applicant respectfully requests reconsideration and withdrawal of the rejections in view of the following discussion.

This response is submitted along with a Request for Continued Examination (RCE).

Claim Rejections Under § 102

On page 3 of the Office Action, claims 1, 3-4, 7, 9-10, 13 and 15-16 are rejected under 35 U.S.C. § 102(e) as anticipated by Morgan (U.S Patent No. 6,968,459). Applicant respectfully submits that Morgan fails to disclose or suggest independent claim 1, because Morgan fails to disclose or suggest all of the limitations recited in claim 1. Applicant respectfully submits that Morgan at least fails to disclose or suggest that only authenticated software and protected applications have access to the protected data, or authentication means arranged to authenticate software provided to the circuitry, as recited in claim 1.

In the present invention, as defined by the amended independent claim 1, the circuitry includes authentication means arranged to authenticate software provided to the circuitry. Protected data and protected applications are located in a storage area. Storage circuit access control means are arranged to enable the processor to access the storage area in which the protected data and protected applications are located when a first processor mode is set (the unsecure mode). When the first processor mode is set only protected applications and authenticated data may access the protected data. The storage circuit access control means are arranged to prevent the processor from accessing the storage area in which protected data are located when a second processor operating mode is set (secure mode), thereby enabling the processor to execute non-verified software downloaded into the circuitry. Thus, the circuit security data that is stored in the storage area of the storage circuit are not accessible.

Morgan generally discloses a secure computing environment in which a computer automatically operates in a **full-access data storage mode**, if detecting a removable storage

device which provides security information. The security information is detected by the computer which then generates a cryptographic key from the storage device related security information. All data written to the storage device is then encrypted utilizing the cryptographic key. Thus, encrypted data is stored on the storage device. In the full-access data storage mode an authorized user is given access to the encrypted data. If the security information is not present on the removable storage device the computer automatically operates in **a restricted access mode** in which the user does not have full access to the encrypted data on the storage device. Furthermore, no encrypted data can be written to the storage device. Therefore, the security information is connected to how the user is allowed to access encrypted data on the storage device. If the security information is available, the full access mode is set, and the encrypted data on the storage device is available. See Morgan column 6, lines 29-32.

In Morgan, the unsecure mode as defined for the present invention must be considered the "normal" operating mode, i.e. when allowing full-access to the circuit security data on the storage area, e.g. the external drive. See Morgan, col. 3 lines 61-67. In the full-access mode, storage management software uses a cryptographic key to encrypt and decrypt the data stream between the computer and the removable storage drive. The cryptographic key is generated by combining one or more of: device specific security information derived from the unique format information of the removable storage device, manufacturing information of the storage device, drive-specific information, such as drive calibration parameters retrieved from the storage device drive, and user specific information. However, the security information of the storage device in Morgan is actually utilized for reading and writing to the storage device. Furthermore, the security information is related to security of the circuitry as it is used for deciding the access mode to the storage device. However, Morgan fails to disclose or suggest that only authenticated software and protected applications have access to said protected data, as recited in claim 1.

In addition, Morgan does not disclose or suggest authentication means arranged to authenticate software provided to the circuitry. In Morgan, for high-security environments the storage manager prevents both read and write access to the storage device when the computer is operating in restricted access mode. See Morgan column 7, lines 13-15. However, the present invention relates to preventing access to the *security data* on a storage circuit, which is not the equivalent to preventing access to the storage device discussed in Morgan.

Furthermore, Morgan does not disclose a mode in which the storage circuit access control means are arranged to prevent the processor from accessing the storage area in which protected data are located when a second processor operating mode is set, thereby enabling the processor to execute non-verified software downloaded into the circuitry, as recited in claim 1. There is no indication from the portions of Morgan referred to in the Office Action about enabling the processor to execute non-verified software downloaded into the circuitry. Instead, Morgan discloses that in restricted-access mode, i.e. when the storage device is not fully accessible, the storage manager configures the storage as a read only drive such that *the user* can read data from the removable disk but cannot write data to the storage (or alternatively the user cannot read data from nor write data to the storage). See Morgan column 7, lines 8-16. In addition, the user is prevented from accessing non-sensitive data within the organization.

Therefore, for at least the reasons discussed above, claim 1 is not disclosed or suggested Morgan. Independent claims 7 and 13 are amended to include limitations similar to those recited in claim 1. Therefore, independent claims 7 and 13 are not disclosed or suggested by Morgan for at least the reasons discussed above with respect to claim 1.

The claims rejected above, and depending from the above mentioned independent claims are not disclosed or suggested by Morgan at least in view of their dependencies.

Claim Rejections Under § 103

On page 4 of the Office Action, claims 2, 6, 8, 12, 14 and 18 are rejected under 35 U.S.C. § 103(a) as unpatentable over Morgan in view of Sato (U.S. Appl. Publ. No. 2001/0055980), and claims 5, 11, and 17 are rejected under 35 U.S.C. § 103(a) as unpatentable over Morgan in view of Ishidera (US Patent 2002/0040442 A1).

Sato is directed to a multi-mode cellular phone terminal supporting a plurality of communication systems, which multi-mode cellular phone terminal comprises a system timer for switching over a plurality of clocks and counting different timings to support a plurality of communications system. Ishidera is directed to a software apparatus which executes processes of software with reduced power consumption at the time of operation on a battery and a recording medium. The apparatus determines whether power saving is needed or not.

The cited references fail to make up for the deficiencies in the teachings of Morgan identified above, and because all of the rejected claims ultimately depend from an independent claim, the claims are not disclosed or suggested by the cited references.

Conclusion

It is respectfully submitted that the present application is in condition for allowance, and such action is earnestly solicited. The undersigned hereby authorizes the Commissioner to charge Deposit Account No. 23-0442 for any fee deficiency required to submit this response.

Respectfully submitted,

Date: 7 July 2008

Keith R. Obert
Attorney for the Applicant
Registration No. 58,051

KRO/kas
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, Connecticut 06468
Telephone:(203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955